Measuring Individuals' Concerns over Collective Privacy on Social Networking Sites

Completed Research Paper

Haiyan Jia
The Pennsylvania State University
University Park, PA
hjia@psu.edu

Heng Xu
The Pennsylvania State University
University Park, PA
hxu@ist.psu.edu

Abstract

With the rise of social networking sites (SNSs), individuals not only disclose personal information but also share private information concerning others online. While shared information is co-constructed by self and others, personal and collective privacy boundaries become blurred. Thus there is an increasing concern over information privacy beyond the individual level. Drawing on the Communication Privacy Management theory, we conceptualize individuals' concerns over collective privacy on SNSs, with three distinctive dimensions—collective information access, control and diffusion, and develop a scale of collective SNS privacy concern (SNSPC) through empirical validation. Structural model analyses confirm the three-dimension structure of collective SNSPC and indicate perceived risk and propensity to value privacy as two antecedents. We discuss key findings, implications and future research directions for theorizing and examining privacy as a collective issue.

Introduction

Social networking sites (SNSs) have been widely adopted and used with diverse purposes and in various scenarios in recent years. Despite the fact that some services such as Yammer and IBM Connections are oriented toward niche communication within a given organization or an enterprise, most of the highly trafficked SNSs such as Facebook, Twitter and Google Plus allow millions of users to connect freely with vast networks of friends and unknown strangers. Individuals create online profiles with personal information ranging from names and gender to their businesses and social connections, which are often shared publicly and open for others to peruse, with the intentions to be found by acquaintances, meet new friends, find new opportunities, and much more.

Such oversharing of the otherwise private information has raised privacy concerns amongst both users and privacy researchers. An increasing amount of effort has been put into evaluating the privacy settings of SNSs (e.g., Gross and Acquisti 2005), examining individuals' information disclosure and privacy protection behaviors (e.g., Young and Quan-Haase 2009), and highlighting potential privacy risks and harms (e.g., Debatin et al. 2009). However, one key aspect of user privacy that is unique to SNSs has been long overlooked. Different from other online contexts such as e-commerce, individuals on SNSs not only disclose information of themselves, but also share information concerning others (e.g., daily schedules with co-workers, group photos with friends, interesting anecdotes of family members, and so forth) inside and outside of their social networks. Likewise, they also have to face the situations where their information is disclosed by their co-workers, friends or family members without their knowledge.

Given that shared content is co-constructed by self and others, and that boundaries between different social circles are often blurred, SNSs bring unprecedented challenges for understanding and managing information privacy. On one hand, the shared information may concern more than one person (e.g., group photos with friends); on the other hand, the control over the access to and reuse of such shared information should be distributed among multiple stakeholders rather than within the original contributors. It seems that the notion of privacy through the individual lens is insufficient to capture the realm of privacy issues on SNSs.

As a result, most recently, privacy scholars have identified the incomprehensiveness of purely studying privacy from the personal perspective in the context of SNSs (e.g., Choi and Jiang, 2013; Shi, Xu and Chen, 2013; Xu, 2012). Instead, they have suggested considering the interpersonal and group perspectives of information privacy. However, there is limited research that has empirically examined if individuals are concerned about the privacy loss of not only of their own, but also of their social ties', in the context of SNSs; nor is there established instrument for capturing individuals' privacy concerns beyond the personal lens.

As a first step to address this gap in existing literature, we conduct an empirical study to examine if individuals are concerned about the privacy loss of their social circles. In what follows, we first provide a review of relevant privacy literature to introduce the construct of privacy concern and existing scales. Drawing on the Communication Privacy Management (CPM) theory (Petronio 2002), we propose that the privacy concerns of SNS users are differentiated at two distinct levels (individual vs. collective) with three informational dimensions (information control, access, and diffusion). This is followed by the development and validation of a preliminary scale for measuring SNS users' individual perceptions of the collective privacy rules and concerns over violations of the collectively held privacy boundaries and expectations. We believe that the development of such a scale is an important first step towards empirically distinguishing the individualistic and the social aspects of privacy concerns, and for measuring different aspects of privacy concerns over collective boundaries on SNSs. We conclude this paper by discussing key findings, research implications, and future research directions.

Theoretical Background

Privacy Concern and Existing Scales

Privacy concern is considered as a central construct in empirical privacy research, as it is often considered as a measurable proxy for the concept of privacy itself (Smith et al., 2011). The privacy literature has documented various approaches for measuring privacy concern. For instance, Smith, Milberg and Burke (1996) developed the scale of measuring Concern for Information Privacy (CFIP) that conceptualizes individuals' privacy concerns with four dimensions: collection of personal information, unauthorized secondary use of information, errors in personal information, and improper access to personal information. Later research argued that the scale of CFIP needed to be adapted in accordance to the advancing of technology. Along this line, Malhotra et al. (2004) defined the specific nature of Internet users' information privacy concerns (IUIPC) with three dimensions—collection of personal information, control over personal information, and awareness of organizational privacy practices. Dinev and Hart (2004) focused on measuring information abuse and unauthorized access as the important components of online privacy concern. Extending CFIP and IUIPC to the context of mobile privacy, Xu et al. (2012) developed a scale of mobile users' privacy concerns, with three dimensions including perceived surveillance, perceived intrusion, and secondary use of personal information.

More specific to the context of SNSs, many privacy scholars have applied the instrument of general Internet privacy concerns to survey studies of SNS users, while including new items that are more relevant to SNS activities, perceptions, or attitudes. For example, Young and Quan-Haase (2009) proposed that SNS users could be particularly concerned about unwanted audience. There is also research indicating that social and communication needs underlie and drive the behaviors of information disclosure on SNSs (Ellison, Steinfield and Lampe 2011). Therefore, privacy expectations vary significantly toward trusted or connected users versus the general public or third parties (Martin 2015). This stream of literature suggests that, in the context of SNSs, the social aspect of privacy considerations play a more significant role than that in other contexts, and therefore conceptualizing SNS privacy through a collective lens is needed for better understanding how privacy perceptions are formed in online social interactions.

The Social Aspect of Privacy Concerns on SNSs

Conceptualizing privacy concern beyond the personal perspective is especially important for understanding information disclosure on SNSs. Different from other scenarios, in the context of SNS, users' perceptions of groups, communities or collectives is one of the key factors that determine their information disclosure. The sense of belonging to the online community or group is likely to enhance

users' sense of trust in the social networking sites, and individuals become more likely to disclose private information to other users of this "imagined community" (Fogel and Nehmad, 2009). The illusion of a closed online community encourages information disclosure on SNSs; while in reality, such online community is often accessible by a wider public (Acquist and Gross, 2006). Studies have shown that individuals reveal personal information on SNSs for social support or information seeking, or for developing and maintaining social relationships (Ellison et al., 2007; 2011).

However, this is not to say that SNS users are not concerned that their private information may be accessed by a wider audience. Rather, they do have an intended and expected audience, which is usually comprised of social categories and groups that have social ties with them (e.g., family members, close friends, and etc). Individuals consider it as socially beneficial to share and exchange private information in given social groups. However, an expectancy violation occurs when people or entities outside of the intended audience, such as potential employers, marketers, corporations or strangers, attain access to their shared information (Stutzman and Kramer-Duffield, 2010). Moreover, users of SNSs are not only concerned about their personal information becoming accessible and viewable to unauthorized parties, but also worried that the privacy of their friends are being exposed and violated. In the context of SNSs, evidence suggests that users are concerned over revealing sensitive topics about friends, losing control over the information that their friends have shared with them, and leaking shared information to unintended others (Choi and Jiang, 2013; Xu, 2012). Finally, information of the entire group or collective, in terms of the existence of such a collective, the social associations that the collective consist, and the interactions within the collective, is also part of this collective level of privacy. According to Bloustein (1976), people have the right to "associate privately with one another" (p.222). In other words, the social aspect of privacy is so much more than the private information of each of the individuals; rather, it entails the characteristics of the collective itself—its members, its purposes, its cohesiveness, its structure and dynamics.

In sum, the entirety of the collective view of privacy encompasses privacy concerns for the violation of an individual's, others' and a group's information privacy, which should be far beyond the personal aspect of privacy analysis in current literature. For this reason, Xu (2012) states that there is an urgent need "to address the acute concerns for collective information privacy in the context of SNSs" (p.1078). In what follows, we introduce the conceptual framework of the collective privacy concerns, which is based on the Communication Privacy Management (CPM) theory (Petronio 2002).

Communication Privacy Management (CPM) Theory

The Communication Privacy Management (CPM) theory (Petronio 1991; 2002) is especially useful for understanding individuals' concerns over both individual and collective privacy. Because this theory "not only gives the option of examining personal privacy boundaries around an individual's information but also allows for the notion of multiple privacy boundaries or collectively held private information (Petronio 2010, p.180)." After individuals share their information online, the shared information moves to a collective domain where collectives (e.g., data subjects and data recipients) manage mutually held privacy boundaries. One of the main contributions of CPM is that the theory recognizes the co-existence of *personal* and *collectively* held privacy boundaries.

Previous research has adopted CPM in online communication contexts such as blogging (Child, Pearson and Petronio, 2009) and family interaction (Child and Petronio, 2011). In both contexts, the presence of others (public or family members as audiences) functions as a significant influence on individuals' self-consciousness (Child et al., 2009) and concern for appropriateness (Child and Agyeman-Budu, 2010), which would consequently affect their privacy rules and disclosure choices. Child et al. (2009) further demonstrate how individuals are concerned about violation of other people's privacy expectations and use the existence of other people as decision criteria when they consider the different aspects of their privacy decision-making.

The existing literature that applies CPM to the computer-mediated communication research only addresses concerns over *personal* privacy (e.g., "I would be upset if my friends shared what's written on my blog"; "I think my parents read my blog regularly"; etc.) in contexts when information is shared and co-owned by others. However, these studies fail to capture the concerns over collective privacy—the collective held boundaries and the distributed responsibilities for keeping the shared information private.

Since SNSs entail information disclosure that invites specific people into a private sphere, recipients of the information experience a sense of co-ownership and responsibility, which contributes to their concerns over the potential privacy loss of their friends' as much as their own, and could determine the extent to which they would exert effort to control and regulate the flow of the shared information. Therefore, it is crucial to examine privacy concerns at both the personal and the collective levels to fully capture what drives individuals to form and coordinate their privacy boundary rules on SNSs.

Individual Concerns over Collective Privacy on SNSs

CPM makes a compelling case for studying individuals' concerns over collective privacy, which calls for the boundary coordination process among both data subjects and data recipients through three boundary coordination rules: coordinating ownership rules, coordinating permeability rules, and coordinating linkage rules (Petronio 2010). These coordination rules "illustrate the modes of change for the dialectic of privacy-disclosure as managed in a collective manner" (Petronio 2002, p.127):

(1) *boundary ownership*, referring to the extent to which the original owner of private information (i.e., data subject) and co-owner (i.e., data recipient) are able to control further possessing or soliciting information (Child et al. 2009; Petronio 2010);

(2) *boundary permeability*, referring to how much others are able to access the shared information within the co-owned privacy boundary (Petronio 2010); and

(3) *boundary linkage*, denoting the associations through which shared information within the co-owned privacy boundary could be reshared and leaked (Petronio 2010).

In this paper, we develop three dimensions of privacy concerns in SNS (*SNS privacy concern* or *SNSPC*), corresponding to the three boundary coordination rules in the CPM theory. Specifically, we argue that: First, users' ownership or co-ownership of shared information will be practically defined in terms of the collective *control* over the shared information, leading towards conflicts regarding who are capable of making decisions about collective boundary of the shared information. Second, the permeability rules will be manifested in the *access* restrictions of the shared information, which determines the closeness and openness of the collective boundary structure. Third, *diffusion* of the shared information beyond the original boundaries will signal the violation of boundary linkage rules. In what follows, we discuss these three dimensions of SNSPC.

Concerns over Collective Information Control

At the personal level, ownership rules capture the extent to which the original owner feels that he/she has right to own private information (Petronio, 2002) and control to make independent decisions about further disclosure (Child et al., 2009). In the SNS context, it often takes shape in the behavior of publishing and sharing of certain private content. As the original owner, individuals may assume that they have the absolute control over their private information and are able to independently regulate access or diffusion of such shared information (Child and Petronio, 2011).

However, such perceptions are challenged as soon as information is shared from the original owner (data subject) to co-owners (data recipients) and/or when the shared information concerns several other parties or stakeholders. In the example of Facebook, collective ownership takes the form of distributed control that designates who (original owner, recipients, stakeholders, etc.) have the capability to regulate the information flow (Fong, Anwar and Zhao, 2009). In these cases, the original owner no longer has sole control over the information; rather, co-owners and stakeholders all are able to make further decisions about information access and diffusion. Thus ownership rules are negotiated among people who have been granted access to the shared information. Overlooking the collectively shared control would potentially leads to conflicts among the co-owners concerns over inability to control one's social sphere (Houghton and Joinson, 2010). Moreover, existing SNS services provide limited options for users to specify who the co-owners are or explicitly negotiate ownership rules (Squicciarini, Xu & Zhang 2010), which may give rise to users' concerns about violating collectively held privacy expectations. Therefore, we posit that concern about the potential loss of collective control, rooted from the coordinating ownership rules in CPM, is an important dimension of SNSPC.

Concerns over Collective Information Access

At the personal level, individuals often create boundary structures to reduce the boundary permeability and the possibility of information leakage; otherwise they may excise less control for a higher degree of permeability (Petronio, 2002). On social networking sites, individuals can modify privacy settings to adjust accessibility of their shared information in order to meet their social, contextual or personal needs (Petronio & Reierson, 2009). They may set their personal profiles as public for the purposes of being able to be contacted and signaling their willingness to meet new friends; they may also limit the access to friends only or to specific groups in order to avoid unsolicited contacts. However, not always will the actual privacy settings be consistent with their privacy expectations (Hoadley et al., 2010). Therefore, individuals may be concerned with unwanted access to their private information by complete strangers or even known friends with whom they do not plan to share such information. They may also have concerns over whether their personal access rules will be maintained once their private information is shared, as existing privacy mechanisms (such as Facebook groups and Google Plus Circles) do not expressively communicate users' desires for privacy controls to the co-owners. The lack of explicit expression of privacy and sharing preferences can easily lead to violations of the boundary permeability rules in the process of information sharing in social networking sites (Squicciarini et al., 2010).

At the collective level, violation of boundary permeability rules is more likely as current SNSs only support individual privacy decisions without offering effective mechanisms for collaborative privacy management among all stakeholders of shared content (Squicciarini et al., 2010). Therefore, one stakeholder can set privacy policy that regulates the access to the shared data while compromising the privacy concerns of other co-owners. Such conditions will trigger concerns over access to the collectively held information boundaries, as the executed privacy policy may only reflect or prioritize the privacy preference of the original owner or some (but not all) co-owners (Swathi et al. 2014). A third party may also obtain and use without permission the shared information that may concern several co-owners, leading towards potential privacy loss of the collective. Therefore, we posit that concern about access to the collectively held information boundaries, rooted from the coordinating permeability rules in CPM, is an important dimension of SNSPC.

Concerns over Collective Information Diffusion

The coordinating linkage rules refer to "the establishment of mutually agreed-upon privacy rules used to choose others who may be privy to the collectively held information" (Jin 2012, p.70). In the SNS context, the coordinating linkage rules involve the establishment of a linkage to become a co-owner of the shared information—the selection of one's social connections to be allowed into the collective privacy boundary (Child et al., 2009). When a linkage is established, the new confidant is expected to assume shared responsibility for protecting the collectively held information boundary. CPM also predicts that the inclusion of a linkage will be followed by disclosure and contribution of the new co-owner to the shared information, further strengthening the cohesiveness of the collective boundary. Personal concern over information diffusion often is triggered by secondary use of personal information, either by unintended users or for unpermitted purposes (Smith et al., 1996; Xu et al., 2012). Individuals are also concerned with information being used out of context, and consequences of such context collapse which may include personal relationship damage (Wang et al. 2013).

More importantly, SNSs bring more opportunities to violate the coordinating linkage rules at the collective level. As information sharing potentially increases the number of information co-owners and stakeholders, it also extend the degree to which information could flow through associations and social relations, with a richer range of possible relational ties and context crossovers (Kane et al. 2012; Hoadley et al., 2010). Therefore, individuals now face the potential new information diffusion through different social networks of all the stakeholders involved. Their concerns over the collective diffusion rules would thus involve not only the structural features of one's personal networks (closeness of networks), but also the extended reach of these social networks and the overall online community (density of networks). Consequently, we believe that concern over the collective information diffusion, rooted from the coordinating linkage rules in CPM, is a complex factor that contributes to SNS users' privacy concerns.

Instrument Development and Validation

Following the conceptual framework outlined above, we develop and validate an instrument to measure individuals' collective privacy concerns in SNSs (Collective SNSPC). The process of our instrument development and validation followed the steps suggested by MacKenzie, Podsakff and Podsakff (2011) in the general context of behavioral research and those outlined by Smith, Milberg and Burke (1996) in the specific context of privacy research.

The process includes three stages. Stage 1 involves specifying the conceptualization and dimensions of the construct, generation of sample items, and assessment of the validity of the items. Stage 2 involves a preliminary examination and an exploratory factor analysis of the instrument items. During this stage, an online survey (N = 304) with Amazon Mechanical Turk participants was conducted to gather empirical data. Stage 3 involves an assessment of the internal validity and the reliability of the instrument. Confirmatory factor analysis is conducted to compare the alternative models of the construct to further confirm the dimensionality of the construct. Further, discriminant validity is tested to verify if individuals' concerns over collective privacy is distinctive from concerns over personal privacy in the SNS context. Finally, test-retest reliability of the instrument is assessed and its generalizability is tested using different populations. During this stage, a second online survey (N = 427) with undergraduate student participants was conducted for data collection.

Stage 1

To specify the dimensions and to establish the instrument, an extensive literature review was conducted. Based on the literature review, the theoretical definition of the *collective SNSPC* was proposed. As discussed earlier, *collective SNSPC* refers to concerns about privacy rule violations (e.g., inappropriate information handling, access and misuse) related to the private information collectively owned by their social networks. To prime participants about the notion of "collective," they were asked to think about "a group of friends" with whom they frequently interact on SNS while answering the questions. Drawing upon the CPM theory, three dimensions were identified as underlying privacy concerns over collective information *control*, *access* and *diffusion*. As shown in Table 1, collective privacy concerns encompass concerns about losing collective control over the shared information, unpermitted information access and diffusion beyond the collectively held boundaries by current stakeholders.

Scale items were sampled from existing empirical literature that measures these two constructs (*Collective* and *Personal SNSPC*) and related concepts. The questionnaire was first presented and judged by 10 graduate students and faculty members at a large university in U.S. to evaluate the items for their applicability to the respective dimensions. After this analysis, the items were further evaluated by using an online survey pretest, where 117 Mechanical Turk participants answered the survey and discussed their reactions to the questionnaire.

Stage 2

To empirically assess the instrument through exploratory methods, an online survey was administered using a sample of 304 Mechanical Turk participants, with an average age of 40, ranging from 18 to 75 years old, and male participants as 41.4% of the sample. The survey was distributed to Mechanical Turk users with two restraints: the users need to (1) currently reside within the United States, and (2) maintain an approval rate of 90% or higher. These restraints were implemented to help ensure obtaining usable and reliable data from a U.S.-based sample (Mason & Suri, 2012; Kittur, Chi & Suh, 2008).

With the empirical data from the Mechanical Turk sample, exploratory factor analysis was conducted and inter-item reliability (Cronbach's alphas) was assessed. For both *personal SNSPC* and *collective SNSPC*, three factors emerged from the 12 items representing three subscales, respectively, as proposed: Access (4 items), Control (4 items), and Diffusion (4 items).

Specifically, for the 12-item scale of Personal SNSPC, the exploratory factor analysis with varimax rotation yielded all factor loadings greater than .60 and the inter-item reliabilities (Cronbach's alpha) greater than .90. The results indicated three dimensions of personal privacy concern, and that the items were sufficiently loaded to the three factors with high inter-item reliabilities.

Table 1. Collective SNS Privacy Concerns (Collective SNSPC)

Factors	**Items**
Please think about you and your social ties—a group of your friends with whom you frequently interact on social networking sites (e.g., Facebook, Twitter, Pinterest, Instagram, etc.), and answer the following questions. *Social Networking Sites (SNSs) such as Facebook provide users with various features to facilitate social connectivity and content sharing. Your shared information may not only reveal your own identity but also connect with your social ties (e.g., tagging a friend in a photo or place checked-in). Likewise, your personal information could be shared by your social ties on SNSs. Regarding the shared information you and your social ties co-manage, please indicate how strongly* ***you and your social ties*** *may agree with the following statements:*	
Control	1. It usually bothers us when we do not have control over who can get access to our conversations on social networking sites. 2. It usually bothers us when we do not have control over which parts of our interactions are displayed on social networking sites. 3. It usually bothers us when we do not have control over decisions about how our information and interactions are collected, used and shared by others. 4. We are concerned that our control over our information and interactions are reduced as a result of oversharing by others.
Access	1. We are concerned that as a result of using social networking sites, others may know more about us than we are comfortable with. 2. We are concerned that as a result of using social networking sites, information about us that we consider private is now more readily available to others than we would want. 3. We are concerned that as a result of using social networking sites, information about us is out there that, if used, would invade our privacy. 4. It bothers us that social networking sites shows everyone a history of our interaction from the past till now.
Diffusion	1. We are concerned that other people may see what we post on social networking sites when we do not intend to. 2. We are concerned that what we share within our group might be seen by others without our knowledge. 3. We are concerned that other people may use what we post on social networking sites for other purposes without notifying us or getting our permission. 4. We are concerned that other people may share what we post on social networking sites with people outside of our networks without getting our permission.

Correspondingly, the preliminary assessment of the 12 items measuring Collective SNSPC yielded conceptually similar dimensions (see Table 2). The items were loaded to the three factors—Collective Access, Collective Control, and Collective Diffusion—as hypothesized, each factor consisting of four items, with all loadings larger than 0.60. The three factors of the collective privacy concern scale also show strong inter-item reliabilities, with Cronbach's alphas larger than 0.90.

One final step of Stage 2 involved model testing to determine if the proposed three-dimension constructs provide the best fit to the data as compared to the alternative plausible models. To accomplish this, the overall model fit statistics of three theoretical plausible models—a unidimensional model, a three-dimensional model, and a model with a second-order construct with three sub-factors—were compared using structural equation modeling program AMOS (Arbuckle, 2013):

1. The *unidimensional model* hypothesizes that all items of collective SNSPC form into a single factor, which accounts for all the variance among the 12 items. Previous research (e.g., Dinev and Hart 2006; Smith et al. 1996) has measured general privacy concern as a unidimensional construct. If this model is accepted, it indicates that it is appropriate to conceptualize collective SNSPC as a single dimension rather than a three-dimension construct.
2. The *three-factor model* hypothesizes that the 12 items of collective SNSPC form into three first-order factors: collective information control, access and diffusion. The assumption of this model is to conceptualize SNS users' collective privacy concerns over three different aspects, and that each of the three aspects are important, independent components in computing an overall score for SNSPC.
3. The *second-order model* hypothesizes that the 12 items of collective SNSPC form into three first-order factors, which are measured by a second-order factor SNSPC. In this model, we consider the first-order factors (i.e. control, access and diffusion) as inter-correlated. Each of the three factors and the second-order factor of SNSPC itself are important in capturing the nature of the entirety of the

construct. If this model is accepted, it indicates that SNSPC is conceptualized as the three factors and the interrelationships among these factors.

Table 2. Factor Analysis of Collective SNS Privacy Concerns

		Component			Cronbach's Alpha
		1	2	3	
Collective Privacy Concern – Access (CPCA)	CPCA1	**.831**			0.947
	CPCA2	**.846**			
	CPCA3	**.837**			
	CPCA4	**.698**			
Collective Privacy Concern – Control (CPCC)	CPCC1		**.846**		0.938
	CPCC2		**.856**		
	CPCC3		**.848**		
	CPCC4		**.665**		
Collective Privacy Concern – Diffusion (CPCD)	CPCD1			**.753**	0.958
	CPCD2			**.782**	
	CPCD3			**.775**	
	CPCD4			**.746**	
Rotation Sum of Squared Loadings	Total	3.632	3.361	3.446	
	% Variance	30.270	28.006	28.716	
	Cumulative Variance	30.270	58.276	86.991	

Model fit statistics including CMIN/DF, CFI and SRMR were calculated to assess the model fit. Comparison of the three models—the one-factor model, the three-factor model, and the second-order model—indicates that the proposed second-order model performs better on the overall model fit statistics than the alternative models for both scales. The second-order model of personal privacy concern yielded better model fit statistics (Table 4), confirming previous research that has conceptualized a CPM-based three-dimensional model of privacy concern in other contexts (e.g., Xu et al., 2012).

For the collective privacy concern scale, comparison of the statistics suggested that the hypothesized second-order model performed better than competing models. As shown in Table 3, the chi-square statistics for all three models were significant, but the significant chi-squares likely resulted from the large sample size. Therefore, CFI and SRMR, which are independent of sample size, were used as indicators of the model fit. The CFI statistics of the second-order model was higher than the other two competing models. The SRMRs were also higher in the competing models than in the hypothesized model. Thus, the comparison shows that the proposed second-order model provided the best fit to the data of all three models compared.

Table 3. Comparison of Three Models of Collective SNSPC.

	One-Factor Model	**Three-Factor Model**	**Second-Order Model**
Chi-square*	1060.106	256.645	229.615
DF	51	51	51
CMIN/DF	20.786	5.032	4.502
CFI	0.822	0.955	0.961
SRMR	0.096	0.053	0.045

*$p < 0.001$ for all models tested.

In sum, the second-order models for both personal SNSPC and collective SNSPC have a CMIN/DF (3.989 and 4.502, respectively) that indicates acceptable model fit (< 5), and both the CFI (0.962 and 0.961, > 0.95) and SRMR (0.069 and 0.045, < 0.08) of the second-order model are better than those for the two alternative models.

To assess the convergent validity of the instrument, further analysis was conducted to determine the degree to which the three sub-factors are correlated (Barki and Hartwick, 1994). Therefore, the correlations between the sub-factors were examined. Results (see intercorrelation results of the collective SNSPC scale in Table 4) indicate that the correlations between the three dimensions are significantly different from zero ($p < 0.05$). This suggests that the three dimensions are not orthogonal and instead measure some aspects of the same construct.

Table 4. Factor Intercorrelation of Three-Factor Model of Collective SNS Privacy Concerns.

Factors	CPCA	CPCC	CPCD
Collective Privacy Concern – Access (CPCA)	1		
Collective Privacy Concern – Control (CPCC)	0.71	1	
Collective Privacy Concern – Diffusion (CPCD)	0.81	0.83	0

Stage 3

Stage 3 included assessments of the internal validity, the generalizability, the discriminant validity and the nomological validity of the instrument. At this stage, an online survey was administered with a sample of 427 undergraduate students at a large university in U.S., aged 18 to 33 (M = 20.1), with 168 (39.3%) female respondents.

Internal Validity and Generalizability. To assess the construct validity, the dimensionality and the generalizability of the instrument, we collected data from a demographically different group and assessed the adequacy of the model fit of the second-order model through confirmatory data analysis (CFA). The results from the undergraduate survey revealed supporting and better performing results, indicating good test-retest reliability of the instrument.

The CFA tests yielded satisfactory model fit statistics for the second-order model of collective SNSPC (see Figure 1). The results of the structural model include: *Chi-square* = 200.32, *DF* = 50, *CMIN/DF* = 4.00, $p < 0.001$; *CFI* = 0.97; *RMSEA* = 0.07; *SRMR* = 0.04. Following recommendations by Hu and Bentler (1999) and MacCallum et al. (1996), the results indicate an acceptable to good model fit (*CMIN/DF* < 5; *CFI* > 0.95; *RMSEA* < 0.08; *SRMR* < 0.08).

Discriminant Validity. To examine the discriminant validity of the collective SNSPC scale and to test if participants distinguish between personal SNSPC and collective SNSPC, a chi-square difference test (Segars, 1997) was conducted, which involves comparison of two models, one in which the two constructs—personal SNSPC and collective SNSPC—are correlated and one in which they are not. The significance of the test result would indicate the discriminant validity of the instrument.

Specifically, confirmatory factor analysis (CFA) was used to compare the two models. In the first model analyzed through CFA, the two constructs were not correlated, whereas in the second one the correlation was allowed. The chi-square different test was significant ($p < 0.001$), indicating that the two constructs present discriminant validity (see detailed results in Appendix B).

Nomological Validity. To examine the instrument's nomological validity, which refers to the extent to which predictions based on the construct are confirmed within a wider theoretical context or a structural model of constructs (Cronbach, 1971), we examined the relationships between some possible antecedents and the construct of collective SNS privacy concern.

Specifically, two theoretically plausible causal variables were assessed, including (1) perceived risk and (2) propensity to value privacy (Smith et al., 2011; Xu et al., 2011). The two variables tested here were suggested in prior research as antecedents that might affect privacy concerns. Appendix C shows the original scales measuring the two variables from the personal perspective, and the newly adapted

instrument that measures *perceived collective privacy risk* and the *collective's propensity to value privacy*.

The structural model of collective SNSPC and its two antecedents yielded sufficient model fit statistics results. Specifically, the structural equation modeling test showed: *Chi-square* = 365.26, *DF* = 128, *CMIN/DF* = 2.85, $p < 0.001$; *CFI* = 0.97; *RMSEA* = 0.06; *SRMR* = 0.04. Figure 2 shows that perceived privacy risk that the collective may experience, and the collective's propensity to value its privacy, are both positively associated with the level of collective SNS privacy concerns.

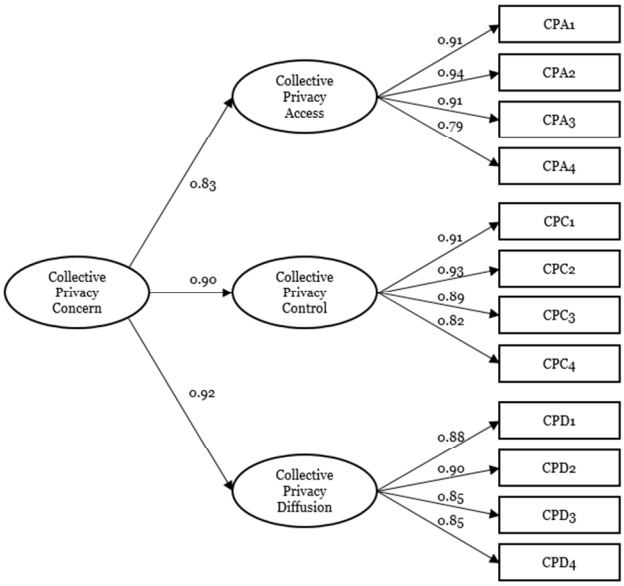

Figure 1. Second-Order Model of Collective SNS Privacy Concern.

Discussion and Conclusion

This paper aims at empirically substantiating the notion of collective privacy concern, and developing and validating an instrument to measure SNS users' individual concerns over collective privacy. The booming popularity of SNSs has brought an additional dimension to the complexity of privacy risks. According to Zittrain (2008), early threats to people's online information privacy came mostly from data stored in government or corporate databases, which he calls Privacy 1.0; yet, with the rise of SNSs, we have transitioned into an era of Privacy 2.0, where the data is generated and shared by individuals, and the "generativity" of SNSs breeds a new generation of privacy problems. Xu (2012) has further extended the notion of Privacy 2.0 to indicate that it is not simply the user generated data that has caused the possible privacy breaches; rather, the networked nature of such user data from users and their social ties, and the uncoordinated actions of individuals (both in terms of information sharing and information management), lead to the new privacy challenge. As Xu (2012) pointed out, in the context of SNSs, keeping data safe and private has become a shared responsibility between users and social connections. That means, even if some user adopts tight privacy settings or is cautious about his or her own information disclosure, the private information could still be leaked or misused due to their friends' ignorance of privacy and security. The widespread of SNSs increases the scope of privacy threats, which emerges as a result of dysfunctional coordination and fosters the awareness of collective privacy risks among SNS users. However, until now, few studies have made systematic attempts to specify privacy concerns from such a collective perspective. This study attempts to fill this gap in the privacy research by examining SNS users' collective privacy concerns and furthering privacy research beyond the scope of privacy as an individualistic concept.

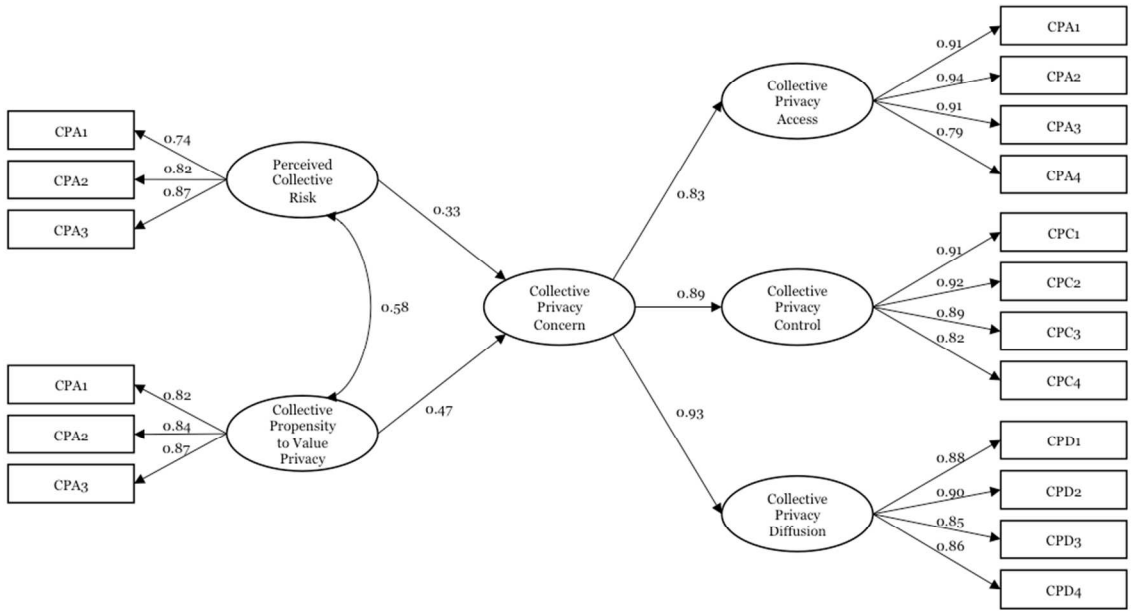

Figure 4. Second-Order Factor Model of Collective SNSPC within its Nomological Network.

Drawing on the CPM theory (Petronio, 2002) and extensive review of the empirical studies of SNS-related privacy concern, we constructed an instrument and empirically tested the three-dimensional measurement of SNSPC scale through a series of online surveys. Exploratory and confirmatory factor analyses have revealed three factors—*collective control*, *access* and *diffusion*—as key dimensions of collective SNSPC. Further analysis indicated that the second-order model of collective SNSPC performed better than the one-factor and three-factor models. The superiority of the fit indices of the second-order SNSPC scale imply that SNS users are concerned with all three aspects of their privacy, and the three dimensions are interdependent in the construction and measurement of collective SNSPC. Further, the scale of SNSPC shows robust results in structural equation models with perceived risk and privacy values as antecedents, both confirming prior research focusing on personal privacy and indicating applicability of the propositions at the collective level as well. Our study yielded both theoretical and practical implications on reconceptualizing the notion of privacy concern, as discussed in the following sections.

Differentiating the Individualistic and the Social Aspects of Privacy Concern

In the development of the collective SNSPC scale, we adopted Bloustein's (1976) proposition that collective privacy is an extension of individual privacy, and considered collective privacy as "an attribute of individuals in association with one another within a group, rather than an attribute of the group itself" (p. 124). This conceptualization lends itself to the operationalization of collective privacy concerns in the form of individuals' concerns for the potential privacy loss experienced by the collective's members. Hence, we were able to measure concerns for collective privacy from individual users' perceptions by asking the extent to which they are concerned about the invasion of collective privacy boundaries and the violation of the different aspects of collective privacy rules. Further, discrimination validity test results (Appendix B) indicated that individuals responded distinctively to privacy concerns regarding their own personal privacy boundary and the privacy boundary of their social groups. The nomological validity test results further confirmed the relationships between collective-level antecedents and collective privacy concerns, indicating that individuals' concerns for collective privacy are strongly influenced by social and group factors such as the collective's susceptibility to privacy risk and collective privacy norms.

In the SNS context, Xu (2012) proposes the transition of the agency of privacy from personal control (the self acts as the control agent to protect one's own privacy) to collective control (a social group acts as the control agent to protect the collective privacy). This proposition assumes that the sharing of private information within a collective privacy boundary is accompanied by the distribution of responsibilities for

protecting the collective privacy among the group members (Xu 2012). Such proposition is also reflected in our results, as the follow-up paired samples t-tests showed higher levels of user concerns over personal privacy than collective privacy (Appendix D). Such findings confirmed the theoretical proposition that users perceive the construction and the management of collective privacy as collaborative processes, and their concern over potential threats to the collective privacy is lowered as they expect to rely on the collective knowledge, skill and power to regulate the collective privacy boundary.

Application of the SNSPC Scales

The new SNSPC scale, with its three dimensions, is deeply rooted in the highly social environment of online social networks. Privacy researchers and website designers will be able to utilize the SNSPC scales to capture users' concerns over collective privacy boundary in such contexts and examine how different aspects of privacy concerns affect user adoption and user experience of the sites. In our data collection, we asked our participants to report their frequency of using a variety of social networking sites and services, and found that several sites were among the frequently used. For instance, when rating the fifteen listed social networking sites and services, 59.4% of the participants self-reported as frequent users (who chose response options from "frequently" to "all the time") of Facebook, 52.7% as frequent users of Instagram, and 50.1% as frequent users of Twitter. Given our goal to capture the collective privacy concerns that are most salient to the participants, they were asked to think about their most frequently used SNS service and the social group with which they most frequently interacted while answering the survey questions. Thus, it is reasonable to expect that findings from this study reflect collective privacy concerns throughout a variety of online social networks and services. Still, the SNSPC scale may not be readily applicable to all social networking sites or applications, and adaptions may be needed especially with new, emerging services and contexts.

Before the widespread of SNSs, information privacy usually concerns one Internet user at a time; if the user is worried about being identified or personal information being misused, they may be able to easily hide their online identity or remove personal information. However, when private information is co-created and disseminated throughout a network of users, personal and absolute control over private information is no longer a reality. Consequences of privacy breaches and data misuse are no longer affecting a single user, but could potentially reveal critical information concerning multiple associated users or a wider group. Therefore, we argue that concerns for information privacy in the SNS context are not only different, but also collective in nature. Comparing to online consumer and ordinary Internet users, SNS users are more prone to privacy threats and intrusion at a higher level beyond their personal data management.

While more websites and Internet applications, from consumer websites to news portals, are integrating social features into their site design and structure, collective SNSPC may make an important contribution to the field of Privacy by Design. The findings from this study could yield practical implications for developing privacy-enhancing mechanisms and policies to mitigate the different aspects of user concerns especially in the collective sphere. Today's highly networked cyberspace calls for our attention to investigating and better understanding how social and group dynamics affect individuals' privacy behaviors and decision-making. Our paper is one of the first to provide empirical evidence on the notion of collective privacy. Future research can extend this work and further examine how individuals' concerns over collective privacy may differentiate in its effect from personal privacy concerns on shaping individuals' privacy management strategies and their online activities such as information disclosure and socialization.

Limitation and Future Work

In generalizing the results of this study, we caution readers to note that the social norms and group characteristics vary in different social networking sites, applications, and services. Thus, we call for future research to further confirm the validity of SNSPC in other emerging social networking applications. Second, although we show satisfactory results in two different samples, we note that the demographic variation between these two groups may be limited. Future studies should test the scale with a more diverse sample and consider group factors and individual idiosyncrasies such as cultural differences, technological competence, and generational differences, etc. Third, the nomological validity of the scale can be better examined in a network of other plausible antecedents and outcomes. Other forms of

empirical study designs such as experimental studies can utilize the instrument to measure actual user responses to various collective privacy threats in different social contexts and scenarios. Future research can investigate how personal and collective privacy concerns may differ and converge under various social and technological influences, producing different psychological and behavioral responses.

While this research constitutes a step toward a better understanding of collective privacy concern in SNS, it raises many questions that need to be addressed in future research. In conclusion, we hope that the ideas and preliminary results put forth in this paper will motivate privacy researchers to move beyond the individual notion of privacy. Further, we hope this paper may serve as a starting point for empirical privacy research to adopt a multi-level approach in conceptualizing privacy and its implications in social interactions, which remains a relatively unexplored area in our field.

Acknowledgements

The authors are grateful to the associate editor and reviewers for their constructive comments on an earlier version of this manuscript. The authors gratefully acknowledge the financial support of the U.S. National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

Appendix: Research Constructs and Measures

Appendix A. Individual Privacy Concerns (Individual SNSPC)

We also captured *personal SNSPC* in this study, which encompass concerns about losing personal control over the private information, unpermitted access to the private information and potential diffusion of the private information.

Factors	Items
Control	• It usually bothers me when I do not have control over who can get access to my personal information on social networking sites. • It usually bothers me when I do not have control over which part of my personal information is displayed on social networking sites. • It usually bothers me when I do not have control over decisions about how my personal information is used and shared by others. • I am concerned that my control over my personal information is reduced as a result of oversharing by others.
Access	• I am concerned that as a result of my using social networking sites, others might know more about me than I am comfortable with. • I am concerned that as a result of my using social networking sites, information about me that I consider private is now more readily available to others than I would want. • I am concerned that as a result of my using social networking sites, information about me is out there that, if used, could invade my privacy. • It bothers me that social networking sites show everyone a history of me from the past till now.
Diffusion	• I am concerned other people might see what I post on social networking sites when I do not intend to. • I am concerned that what I share with a small group of friends on social networking sites might be seen by others without my knowledge. • I am concerned that other people might use what I post on social networking sites for other purposes without notifying me or getting my permission. • I am concerned that other people might share what I post on social networking sites with people outside of my networks without getting my permission.

Appendix B. Chi-Square Difference Test between Personal and Collective SNSPC.

Model 1	**Model 2**
Chi-square = 4092.043 Degrees of freedom = 252 Probability level = .000	Chi-square = 3673.631 Degrees of freedom = 251 Probability level = .000
$X_1 - X_2 = 418.412$	
$df_1 - df_2 = 1$	

Appendix C. Measurement of Perceived Risk and Propensity to Value Privacy.

Factor	**Individual-Level Measurement**	**Collective-Level Measurement**
Perceived Risk *(Adapted from the RISK scale in Xu et al. 2011)*	1. In general, it is risky to share my personal information online. 2. It is likely that others will use my personal information inappropriately online. 3. Sharing my personal information online will lead to many unexpected problems.	1. In general, it is risky for my friends and me to share our information and interaction on social networking sites. 2. It is likely that others will use what we post online inappropriately. 3. Sharing information and interactions on social networking sites will lead to many unexpected problems for my friends and me.
Propensity to Value Privacy *(Adapted from the DTVP scale in Xu et al. 2011)*	1. I am very sensitive about the way social networking sites handle my personal information. 2. To me, it is the most important thing to keep my information privacy. 3. I tend to be very concerned about threats to my information privacy.	1. As a group, we are very sensitive about the way social networking sites handle our information and interaction. 2. To my friends and me, it is the most important thing to keep our information privacy. 3. As a group, we tend to be very concerned about threats to our information privacy.

Appendix D. Paired Samples T-Test Results.

		Mean	**SD**	**t**	**DF**	**p**
Pair 1	Personal Privacy Access	4.552	1.470	2.485	730	0.006
	Collective Privacy Access	4.433	1.421			
Pair 2	Personal Privacy Control	4.913	1.350	5.827	730	0.000
	Collective Privacy Control	4.645	1.402			
Pair 3	Personal Privacy Diffusion	4.555	1.426	4.386	730	0.000
	Collective Privacy Diffusion	4.353	1.412			

References

Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, pp. 36-58, Springer Berlin Heidelberg.

Arbuckle, J. L. 2013. *IBM® SPSS® Amos™ 22 User's Guide*. Chicago, IL: IBM.

Bandura, A. 2001. Social Cognitive Theory: An Agentic Perspective. *Annual Review of Psychology* (52:1), pp. 1-26.

Bloustein, E.J. 1976. "Group privacy: The Right to Huddle," *Rutgers Law Journal* (8), pp. 219-283.

Child, J.T., and Agyeman-Budu, E.A. 2010." Blogging Privacy Management Rule Development: The Impact of Self-Monitoring Skills, Concern for Appropriateness, and Blogging Frequency," *Computers in Human Behavior* (26:5), pp. 957-963.

Child, J.T., Pearson, J.C., and Petronio, S. 2009. "Blogging, Communication, and Privacy Management: Development of the Blogging Privacy Management Measure," *Journal of the American Society for Information Science and Technology* (60:10), pp. 2079-2094.

Child, J.T., and Petronio, S. 2011. "Unpacking the Paradoxes of Privacy in CMC Relationships: The Challenges of Blogging and Relational Communication on the Internet," In K. B. Wright and L. M. Webb (Eds.), *Computer-Mediated Communication in Personal Relationships*, pp. 21-40.

Choi, C.F., and Jiang, Z. 2013. "Trading Friendship for Value: An Investigation of Collective Privacy Concerns in Social Application Usage," *Proceedings of Thirty Fourth International Conference On Information Systems (ICIS 2013)*, Milano, Italy, pp. 1-10.

Cronbach, L.J. 1971. "Test Validation," In R. L. Thomdike (Ed.), *Educational measurement (2nd Ed.).* Washington DC: American Council on Education.

Debatin, B., Lovejoy, J.P., Horn, A.K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*," Journal of Computer-Mediated Communication* (15:1), pp. 83-108.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Ellison, N. B., Steinfield, C., and Lampe, C. 2011. "Connection Strategies: Social Capital Implications of Facebook-Enabled Communication Practices," *New Media & Society* (13:6), pp. 873-892.

Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication* (12:4), pp. 1143-1168.

Fogel, J., and Nehmad, E. 2009. "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns," *Computers in human behavior* (25:1), pp. 153-160.

Fong, P.W., Anwar, M., and Zhao, Z. 2009. "A Privacy Preservation Model for Facebook-Style Social Network Systems," *Proceedings of the European Symposium on Research in Computer Security (ESORICS 2009), Saint-Malo, France*, pp. 303-320, Springer Berlin Heidelberg.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 71-80.

Hoadley, M. C., Xu, H., Lee, J., Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp. 50-60.

Houghton, D.J., and Joinson, A. N. 2010. "Privacy, Social Network Sites, and Social Relations," *Journal of Technology in Human Services* (28:1-2), pp. 74-94.

Hu, L.T., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.

Jin, S.A.A. 2012. "To Disclose or Not to Disclose, That Is the Question': A Structural Equation Modeling Approach to Communication Privacy Management in E-Health," *Computers in Human Behavior* (28:1), pp. 69-77.

Kane, G.C., Alavi, M., Labianca, G.J., and Borgatti, S. 2012. "What's Different about Social Media Networks? A Framework and Research Agenda," *MIS Quarterly* (38:1), pp. 274-304.

Kittur, A., Chi, E.H., and Suh, B. 2008. "Crowdsourcing User Studies with Mechanical Turk," *Proceedings of The SIGCHI Conference On Human Factors In Computing Systems*, pp. 453-456.

MacCallum, R.C., Browne, M.W., and Sugawara, H.M. 1996. "Power Analysis and Determination of Sample Size for Covariance Structure Modeling," *Psychological methods* (1:2), pp. 130-149.

MacKenzie, S.B., Podsakoff, P.M., and Podsakoff, N.P. 2011." Construct Measurement and Validation Procedures In MIS And Behavioral Research: Integrating New And Existing Techniques," *MIS Quarterly* (35:2), pp. 293-334.

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), 336-355.

Martin, K. 2015. "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics*, forthcoming.

Mason W., and Suri, S. 2012. "Conducting Behavioral Research on Amazon's Mechanical Turk," *Behavior Research Methods* (44:1), 1-23.

Petronio, S. 1991. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples," *Communication Theory* (1:4), pp. 311-335.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

Petronio, S. 2010. "Communication Privacy Management Theory: What Do We Know about Family Privacy Regulation?" *Journal of Family Theory & Review* (2:3), pp. 175-196.

Petronio, S., and Reierson, J. 2009. "Regulating the Privacy of Confidentiality: Grasping the Complexities through Communication Privacy Management Theory," In T. Afifi and W. Afifi (Eds.), *Uncertainty, information management, and disclosure decisions: Theories and applications*, pp. 365-383, Routledge.

Segars, A. 1997. "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research", *Omega* (25:1), pp. 107-121.

Shi, P., Xu, H., and Chen, Y. 2013. "Using Contextual Integrity to Examine Interpersonal Information Boundary on Social Network Sites," *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI), Paris, France, pp. 35-38.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Smith, H.J., Milberg, J.S., and Burke, J.S. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Squicciarini, C. A., Xu, H., and Zhang, X. 2011. "CoPE: Enabling Collaborative Privacy Management in Online Social Networks," *Journal of the American Society for Information Science and Technology* (62:3), pp. 521-534.

Stutzman, F., and Kramer-Duffield, J. 2010. "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2010)*, pp. 1553-1562.

Swathi, G., Radharani, A., and Babu, K.M. 2014. "Self-Controlled Privacy Policy for Online Social Networks Using Multi-Party Access Control," *The International Journal of Computer Science Information and Engineering Technology* (4:3).

Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A., and Cranor, L.F. 2013. "Privacy Nudges for Social Media: An Exploratory Facebook Study," *Proceedings of the 22nd International Conference on World Wide Web Companion*, pp. 763-770.

Xu, H. 2012. "Reframing Privacy 2.0 in Online Social Network," *University of Pennsylvania Journal of Constitutional Law* (14:4), pp. 1077-1102.

Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M. 2012. "Measuring Mobile Users' Concerns for Information Privacy," *Proceedings of 29th Annual International Conference on Information Systems (ICIS)*, Orlando, FL.

Young, A. L., and Quan-Haase, A. 2009. "Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook," *Proceedings of the Fourth International Conference on Communities and Technologies*, pp. 265-274.

Zittrain, J. 2008. "Privacy 2.0," *The University of Chicago Legal Forum*, pp. 65-120.